The Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

What is claimed is:

1.- 32. (Canceled)

33. (Currently Amended) A method of loading data into a mobile terminal data comprising payload data and header data, the method comprising the steps of:

receiving a header message ~~including the header data~~ from a loading station by a mobile terminal wherein the header message includes the header data having a cryptographic data item including a cryptographic checksum based on a message digest of the message calculated by a hash function;

verifying the received header data by the mobile terminal;

receiving the payload data, if the header data is verified successfully;

accepting the payload data by the mobile terminal conditioned on a verification process based on the header data, wherein the payload data is divided into a number of blocks of payload data and the blocks of payload data do not carry authentication information;

wherein receiving the payload data further comprises receiving a number of payload messages each including one of the number of blocks of payload data; and

wherein accepting the payload data further comprises accepting each of the blocks of payload data by the mobile terminal conditioned on a cryptographic verification process based on a corresponding one of a number of received message digests and accepting the payload data conditioned on a verification of a received message digest calculated from a combination of all blocks of payload data.

34. (Previously Presented) The method according to claim 33 wherein the number of message digests received comprises at least one of the sequence of message digests received as a part of the header message.

35. (Previously Presented) The method according to claim 33 wherein the step of accepting each of the blocks of payload data further comprises the step of storing in a storage medium said accepted block of payload data.

36. (Previously Presented) The method according to claim 35 wherein the storage medium is divided into a number of storage blocks each having a predetermined size; and each of the number of blocks of payload data have a block size corresponding to the size of storage blocks.

37. (Previously Presented) The method according to claim 36 wherein the payload data comprises an update of existing data loaded in the mobile terminal and the method further comprises the step of only loading the blocks of payload data which differ from a corresponding block of the existing data.

38. (Previously Presented) The method according to claim 33 wherein each of the message digests is generated from the corresponding block of payload data and from the header message.

39. (Previously Presented) The method according to claim 33 wherein the cryptographic verification process used in the step of accepting a first block of payload data received after a second block of payload data is further based on a result of a cryptographic verification process used in a previous step of accepting the second block of payload data.

40. (Previously Presented) The method according to claim 33 wherein the first cryptographic data item includes a first message digest encrypted with a private key

of an authority and the step of accepting the data by the mobile terminal further comprises the steps of:

calculating a second message digest of. the received header data and the received payload data;

decrypting the first message digest with a public key of said authority; and

comparing the decrypted first message digest with the calculated second message digest.

41. (Previously Presented) The method according to claim 33 wherein the header data further comprises a signed key to be used in the verification process by the mobile terminal as a public key of the authority distributing the payload data.

42. (Previously Presented) The method according to claim 33 wherein the header data further comprises a second cryptographic data item, and the step of verifying the header data further comprises the step of performing a cryptographic verification of the header data based on the second cryptographic data item.

43. (Previously Presented) The method according to claim 33, the method further comprising the step of processing the payload data conditioned on the step of accepting the data by the mobile terminal.

44. (Previously Presented) The method according to claim 43 wherein the payload data is received in a compressed for; and the step of processing further comprises the step of decompressing the payload data.

45. (Previously Presented) The method according to claim 33, the method further comprises the step of sending a request for receiving the payload data to the loading station conditioned on a result of the step of verifying the header data.

46. (Previously Presented) The method according to claim 33 wherein the payload data comprises program code means.

47. (Previously Presented) The method according to claim 33 wherein the payload data comprises a software patch.

48. (Currently Amended) A method of uploading data into a mobile terminal, the method comprising the steps of:

transmitting the data by a loading station to the mobile terminal, the data comprising payload data and header data for use by the mobile terminal in a verification process of the header data; wherein transmitting the data further comprises the step of:

transmitting a header message ~~including the header data~~ to be verified by the mobile terminal before transmitting at least a first payload message including the payload data wherein the header message includes the header data having a cryptographic data item including a cryptographic checksum based on a message digest of the message calculated by a hash function; and

allowing the mobile terminal to reject reception of the payload data;

dividing the payload data into a sequence of blocks of payload data, wherein the blocks of payload data do not carry authentication information;

generating a sequence of message digests, each message digest being related to a corresponding one of the number of blocks of payload data, wherein one message digest is calculated from a combination of all blocks of payload data; and

transmitting the sequence of message digests and a number of payload messages each including one of the number of blocks of payload data.

49. (Previously Presented) The method according to claim 48, the method further comprising the steps of:

receiving a request from the mobile terminal for transmitting the payload data; and

transmitting the payload data to the mobile terminal in response to the received request.

50. (Previously Presented) The method according to claim 48, further comprising the steps of:

processing the payload data to be uploaded into the mobile terminal;

generating a cryptographic data item for the processed payload data; and

transmitting the cryptographic data item as a part of the header data.

51. (Previously Presented) The method according to claim 48, wherein the step of generating a sequence of message digests further comprises the step of generating each of the message digests from a corresponding block of payload data and from the header message.

52. (Previously Presented) The method according to claim 48, wherein the step of transmitting the sequence of message digests further comprises the step of transmitting at least one of the sequence of message digests as a part of the .header message.

53. (Previously Presented) The method according to claim 48, wherein the payload data comprises an update of existing data loaded in the mobile terminal; and the method further comprises the step of only transmitting blocks of payload data which differ from a corresponding block of the existing data.

54. (Currently Amended) A system for loading data into a mobile terminal, the system comprising:

a loading station; and

a mobile terminal;

the loading station including first transmitting means for transmitting data to the mobile terminal, the data comprising payload data and header data wherein the loading

station is adapted to transmit a header message ~~including the header data~~ before transmitting the payload data wherein the header message includes the header data having a cryptographic data item including a cryptographic checksum based on a message digest of the message calculated by a hash function;

the mobile terminal including first receiving means for receiving said data from the loading station; and

processing means adapted to accept the data conditioned on a verification process based on the header data[[;]], wherein the mobile terminal is adapted to receive the header message from the loading station, to verify the received header data and to cause the first receiving means to receive the payload data, if the header data is verified successfully;

the loading station operable to divide the payload data into a sequence of blocks of payload data, wherein such blocks of payload data do not carry authentication information, generate a sequence of message digests, each message digest being related to a corresponding one of the number of blocks of payload data, wherein one message digest is calculated from a combination of all blocks of payload data, and transmit the sequence of message digests and a number of payload messages each including one of the number of blocks of payload data;

the mobile terminal operable to receive the number of message digests the number of payload messages, accept each of the blocks of payload data conditioned on a cryptographic verification process based on a corresponding one of the message digests and accept the payload data conditioned on a verification of the message digest calculated from a combination of all blocks of payload data.

55. (Currently Amended) A mobile terminal comprising:

receiving means for receiving data from a loading station, the data comprising payload data and header data, the receiving means operable to receive a header message ~~including the header data~~ from the loading station wherein the header message includes header data having a cryptographic data item including a

cryptographic checksum based on a message digest of the message calculated by a hash function; and

processing means operable to accept the received data conditioned on a verification process based on the header data wherein the processing means is further adapted to verify the received header data and to cause the receiving means to receive the payload data if the header data is verified successfully;

wherein the payload data is divided into a number of blocks of payload data, wherein such blocks of payload data do not carry authentication information;

the receiving means operable to receive a number of payload messages each including one of the number of blocks of payload data; and

the processing means operable to accept each of the blocks of payload data by the mobile terminal conditioned on a cryptographic verification process based on a corresponding one of a number of received message digests and accept the payload data conditioned on a verification of a received message digest calculated from a combination of all blocks of payload data.

56. (Currently Amended) A loading station for uploading data into a mobile terminal, the loading station comprising:

transmitting means for transmitting data to a mobile terminal, the data comprising payload data and header data for use by the mobile terminal in a verification process when accepting the data, wherein the transmitting means is further operable to transmit a header message ~~including the header data~~ to be verified by the mobile terminal before transmitting the payload data, allowing the mobile terminal to reject reception of the payload data wherein the header message includes the header data having a cryptographic data item including a cryptographic checksum based on a message digest of the message calculated by a hash function;

the loading station further operable to:

divide the payload data into a sequence of blocks of payload data[[,]] wherein such blocks of payload data do not carry authentication information;

generate a sequence of message digests, each message digest being related to a corresponding one of the number of blocks of payload data, wherein one message digest is calculated from a combination of all blocks of payload data; and

transmit the sequence of message digests and a number of payload messages each including one of the number of blocks of payload data.

57. (Previously Presented) The loading station according to claim 56, wherein the loading station comprises a first device including a secure memory for storing a private key, and second processing means for generating a cryptographic data item; and

a second device comprising second processing means for generating the header data including the generated cryptographic data item.

58. (Previously Presented) The loading station according to claim 57, wherein the first device is a smart card.

59. (Currently Amended) A computer program comprising program code means embodied on a computer-readable medium adapted to, when executed data processing device, perform the steps of:

receiving a header message ~~including the header data~~ from a loading station by a mobile terminal wherein the header message includes the header data having a cryptographic data item including a cryptographic checksum based on a message digest of the message calculated by a hash function;

verifying the received header data by the mobile terminal;

receiving the payload data, if the header data is verified successfully;

accepting the data by the mobile terminal conditioned on a verification process based on the header data, wherein the payload data is divided into a number of blocks of payload data and such blocks of payload data do not carry authentication information;

wherein receiving a header message further comprises receiving a number of payload messages each including one of the number of blocks of payload data; and

wherein accepting the data further comprises accepting each of the blocks of payload data by the mobile terminal conditioned on a cryptographic verification process based on a corresponding one of a number of received message digests and accepting the payload data conditioned on a verification of a received message digest calculated from a combination of all blocks of payload data.

60. (Previously Presented) The computer program according to claim 59 wherein the data processing device is a mobile terminal.

61. (Previously Presented) The computer program according to claim 59 wherein the data processing device is a loading station.

***